

PRIME INJECTIONS AND QUASIPOLARITIES

OCTAVIO A. AGUSTÍN-AQUINO

ABSTRACT. Let π be a prime number, $\iota : \mathbb{Z}_n \rightarrow \mathbb{Z}_{\pi n}$ the canonical injection and $e^u.v \in \mathbb{Z}_n \ltimes \mathbb{Z}_n^\times$ and $e^w.r \in \mathbb{Z}_{\pi n} \ltimes \mathbb{Z}_{\pi n}^\times$. Suppose an element $e^u.v \in \mathbb{Z}_n \ltimes \mathbb{Z}_n^\times$ is seen as an automorphism of \mathbb{Z}_n by $e^u.v(x) = vx + u$; then $e^u.v$ is a *quasipolarity* if it is an involution without fixed points. In this brief note we prove sufficient conditions such that $(e^w.r) \circ \iota = \iota \circ (e^u.v)$, where $e^w.r$ and $e^u.v$ are quasipolarities.

1. INTRODUCTION

Suppose $e^u.v \in \mathbb{Z}_n \ltimes \mathbb{Z}_n^\times$ acts on \mathbb{Z}_n by the action

$$e^u.v(x) = vx + u.$$

This action extends naturally to an action on $2^{\mathbb{Z}_n}$ in a pointwise manner. A *marked strong dichotomy* is a subset $D \subseteq \mathbb{Z}_{2k}$ such that there is a unique $p = e^u.v$ such that

$$p(D) = \mathbb{Z}_{2k} \setminus D.$$

The element p is called the *polarity* of D . It is easily seen that, if we regard p as a automorphism of \mathbb{Z}_{2k} , we have $p^2 = \text{Id}_{\mathbb{Z}_{2k}}$ and it has no fixed points. Any $p = e^u.v$ with these properties is called a *quasipolarity*.

In [2, Ch. 4] these constructions were studied in the context of the mathematical theory of counterpoint proposed by Guerino Mazzola, and it was shown that, whenever

- (1) there is a strong dichotomy in \mathbb{Z}_{2k} with polarity p and,
- (2) there is a quasipolarity in $p' \in \mathbb{Z}_{4k}$ such that $\iota \circ p = p' \circ \iota$ (where $\iota : \mathbb{Z}_{2k} \rightarrow \mathbb{Z}_{4k}$ is the canonical injection),

then p' is the polarity of a marked strong dichotomy in \mathbb{Z}_{4k} .

If we were to generalize this result for canonical injections $\iota : \mathbb{Z}_n \rightarrow \mathbb{Z}_{\pi n}$, where π is a prime number, we would need first to find the conditions such that $\iota \circ p = p' \circ \iota$. This is the aim of the following note.

2000 *Mathematics Subject Classification.* 11A05, 11A07.

Key words and phrases. Quasipolarities, prime injection.

2. STATEMENT OF THE MAIN THEOREM

Remark 2.1. We use the following notation, taken from [3]: $a \perp b$ means that a is coprime with b , and $a \setminus b$ means that a divides b .

Suppose $e^u \circ v$ is a quasipolarity. In [1] it is proved that u can be taken as $\frac{n}{\gcd(v+1, n)}$, where v is understood as the minimum representative of its equivalence class in \mathbb{Z}_{2k} . Our interest is to find the conditions such that there exists a quasipolarity $e^w \circ r : \mathbb{Z}_{\pi n} \rightarrow \mathbb{Z}_{\pi n}$ which renders commutative the following square:

$$(1) \quad \begin{array}{ccc} \mathbb{Z}_n & \xrightarrow{\iota} & \mathbb{Z}_{\pi n} \\ e^u \circ v \downarrow & & \downarrow e^w \circ r \\ \mathbb{Z}_n & \xrightarrow{\iota} & \mathbb{Z}_{\pi n}. \end{array}$$

We have the following result.

Theorem 2.2. *Let n be an even number, v an involution modulo n , $k = \frac{v^2-1}{n}$ and $u = \frac{n}{\gcd(v+1, n)}$. If either $\gcd(\pi, 2v) \setminus k$ or $\pi \setminus n$, then there exists t such that $r = v + nt$ is an involution modulo πn . In that case and if $\frac{r^2-1}{\pi n}$ is even, then $e^w \circ r$ is a quasipolarity with $w = \pi u$ and the diagram (1) commutes.*

3. PROOF OF THE MAIN THEOREM

We begin noting that for the square (1) to commute it is necessary and sufficient that

$$w \equiv \pi u \pmod{\pi n}, \quad \pi r \equiv \pi v \pmod{\pi n}.$$

The second congruence is equivalent to $\pi(r - v) = \pi nt$ for some integer t . Hence $r - v = nt$ and

$$r = v + nt.$$

Let v is an involution in \mathbb{Z}_n . We want r to be an involution. We see that

$$\begin{aligned} (v + nt)^2 &= v^2 + 2vnt + n^2t^2 \\ &= 1 + kn + 2vnt + n^2t^2 \\ &= 1 + (k + 2vt + nt^2)n, \end{aligned}$$

so for $(v + nt)$ to be an involution is necessary and sufficient that $\pi \setminus (k + 2vt + nt^2)$. In other words, t is the solution of the quadratic congruence

$$(2) \quad nt^2 + 2vt + k \equiv 0 \pmod{\pi}.$$

We distinguish two cases. If $\pi \nmid n$, then it is enough to solve for t the linear congruence

$$2vt \equiv -k \pmod{\pi}.$$

Such a congruence is solvable if and only if $\gcd(\pi, 2v) \mid k$. Note that if $\pi = 2$, this condition simply means that k must be a multiple of 2.

If $\pi \mid n$, the quadratic congruence is unavoidable. Fortunately, $2n \perp \pi$ so, in order to solve it, we rewrite (2) to obtain

$$(2nt + 2v)^2 \equiv 4v^2 - 4nk \pmod{\pi}$$

which reduces to

$$(nt + v)^2 \equiv v^2 - nk \equiv 1 + nk - nk \equiv 1 \pmod{\pi}.$$

Since 1 is always a quadratic residue, we deduce that $t = n^{-1}(\pm 1 - v)$ where n^{-1} is the inverse of n modulo π .

Suppose now that we have found a t such that $r = v + tn$ is an involution. For there exists w such that $e^w \circ r$ is a quasipolarity, it is necessary and sufficient to check that

$$(3) \quad 2 \frac{\pi n}{\gcd(v + nt + 1, \pi n)} = \gcd(v + nt - 1, \pi n).$$

If (3) is true, we can choose

$$(4) \quad w = \frac{\pi n}{\gcd(v + nt + 1, \pi n)}.$$

Let us begin. Note that

$$\frac{v + nt - 1}{2} \perp \frac{v + nt + 1}{2}$$

and

$$\gcd(v + nt \pm 1, \pi n) = 2 \gcd\left(\frac{v + nt \pm 1}{2}, \pi \frac{n}{2}\right)$$

thus

$$\begin{aligned} \gcd(v + nt + 1, \pi n) \gcd(v + nt - 1, \pi n) &= 4 \gcd\left(\frac{(v + nt)^2 - 1}{4}, \pi \frac{n}{2}\right) \\ &= 4 \gcd\left(\frac{1 + k'\pi n - 1}{4}, \pi \frac{n}{2}\right) \\ &= 2 \gcd\left(\frac{k'\pi n}{2}, \pi n\right) \\ &= 2\pi \gcd\left(k' \frac{n}{2}, n\right). \end{aligned}$$

Observing that

$$\gcd\left(k' \frac{n}{2}, n\right) = n$$

holds if and only if $2 \nmid k'$, it follows that (3) holds if and only if $2 \nmid k'$, where $k' = \frac{r^2-1}{\pi n}$.

To finish, we show that once $e^w \circ r$ is an involution such that $r\pi \equiv v\pi \pmod{\pi n}$ and w is given by (4), it is true that w equals πu and thus the diagram (1) commutes. In case $\pi \nmid (v + tn + 1)$, then

$$\gcd(v + tn + 1, \pi n) = \gcd(v + tn + 1, n) = \gcd(v + 1, n)$$

which means that

$$(5) \quad w = \frac{\pi n}{\gcd(v + tn + 1, \pi n)} = \frac{\pi n}{\gcd(v + 1, n)} = \pi u.$$

Assume now the alternative case $\pi \nmid (v + tn + 1)$. Then any divisor d of $\frac{v+tn+1}{\pi}$ and n is also a divisor of $v + 1$, because $v + 1$ is a linear combination of them:

$$v + 1 = \pi \frac{v + tn + 1}{\pi} - tn.$$

It follows that

$$\gcd\left(\frac{v + tn + 1}{\pi}, n\right) \mid \gcd(v + 1, n)$$

or, equivalently,

$$\gcd(v + 1, n) = \gcd\left(\frac{v + tn + 1}{\pi}, n\right) \pi = \gcd(v + tn + 1, \pi n).$$

The missing factor is π because any common factor d of $v + 1$ and n divides the linear combination $(v + 1) + tn$ and also $\frac{(v+1)+tn}{\pi}$, as long as $d \perp \pi$ or $d = \pi^{\lambda-1}$, where π^λ is the greatest power of π that divides both $v + tn + 1$ and n . In conclusion, equation (5) is true again, and the proof concludes.

Example 3.1. The affine map $e^2 \circ 5 : \mathbb{Z}_{12} \rightarrow \mathbb{Z}_{12}$ is a quasipolarity. Let $\pi = 2$ and $k = \frac{5^2-1}{12} = 2$. Since $2 \nmid k$, there exists a t such that $5 + 12t$ is an involution in \mathbb{Z}_{24} . Using the proof of the theorem, t is the solution of

$$0 \equiv 2 \cdot vt \equiv -k \equiv -2 \equiv 0 \pmod{2},$$

thus t can be chosen arbitrarily. If we choose $t = 0$, $k' = \frac{5^2-1}{24} = 1$ is not even. If $t = 1$, then $r = 5 + 12 = 17$ and $k' = \frac{17^2-1}{24} = 12$ is even and $w = \pi u = 2 \cdot 2 = 4$. Hence $e^4 \circ 17 : \mathbb{Z}_{24} \rightarrow \mathbb{Z}_{24}$ is a quasipolarity such that (1) commutes.

If now we take $\pi = 5$, we have $5 \nmid 12$, so $t = 3(\pm 1 - 5) \bmod 5 = \pm 3$. If we choose $t = 3$, we get $r = 5 + 2 \cdot 12 = 29$ and it is such that $\frac{r^2-1}{60} = 14$ is even, so $e^{10} \circ 29 : \mathbb{Z}_{60} \rightarrow \mathbb{Z}_{60}$ satisfies (1).

OCTAVIO ALBERTO AGUSTÍN AQUINO
UNIVERSIDAD DE LA CAÑADA
INSTITUTO DE FARMACOBIOLOGÍA
CARRETERA TEOTITLÁN-NANAHUATIPAN S/N
TEOTITLÁN DE FLORES MAGÓN, OAXACA
MÉXICO
octavioalberto@unca.edu.mx

REFERENCES

1. Octavio Agustin-Aquino, *Antichains and counterpoint dichotomies*, Contributions to Discrete Mathematics **7** (2012), no. 2, 97–104.
2. Octavio A. Agustín-Aquino, *Extensiones microtonales de contrapunto*, Ph.D. thesis, Universidad Nacional Autónoma de México, 2011.
3. Ronald L. Graham, Donald E. Knuth, and Oren Patashnik, *Concrete mathematics*, Addison-Wesley, 1994.